IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	ELLINGSON
Docket:	13481.1US01
Title:	SYSTEM AND METHOD FOR IDENTITY VERIFICATION

CERTIFICATE UNDER 37 CFR 1.10
'Express Mail' mailing label number: EL674896113US
Date of Deposit. October 5, 2000
I hereby certify that this paper or fee is being deposited with the United States Postal Service 'Express Mail Post Office To Addressee' service under 37 CFR 1 10 and is addressed to the Assistant Commissioner for Patents, Washington, D.C 20231

By. Linda McCormick
Name. Linda McCormick

BOX PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

We are transmitting herewith the attached:

☒ Transmittal sheet, in duplicate, containing Certificate under 37 CFR 1.10.
☒ Utility Patent Application: Spec. 23 pgs; 25 claims; Abstract 1 pg.:
☒ 10 sheets of formal drawings
☒ Small entity status will be established at a later date
☒ An unsigned Combined Declaration and Power of Attorney
☒ Return postcard
☒ **PAYMENT OF THE FILING FEE IS BEING DEFERRED.**

MERCHANT & GOULD P.C.
P.O. Box 2903, Minneapolis, MN 55402-0903
(612) 332-5300

By: John Albrecht
Name: John W. Albrecht
Reg. No.: 40,481
Initials: JWA:PSTtdm

23552
PATENT TRADEMARK OFFICE

(PTO TRANSMITTAL - NEW FILING/DEFERRED FEES)

M&G No. 13481.1US01

SYSTEM AND METHOD FOR IDENTITY VERIFICATION

Related Applications

This application claims the benefit of provisional application, U.S. Serial No. 60/157,889, filed on October 6, 1999, entitled "Identity Verifier", by Robert E. Ellingson.

Technical Field

The present invention relates to identity verification. More particularly, the present invention relates to a system and method for verifying the identity of a registered user.

Background of the Invention

Identity crimes are a significant problem in society. Identity crimes include identity theft, identity fraud, identity cloaking, check counterfeiting, and other crimes. Some specific examples of identity crimes include credit card theft, check theft, medicare fraud, ATM card theft, minors using fake identifications to obtain admittance to a bar or adult-only Internet sites. Many other examples of identity crimes abound around us. Despite new laws designed to combat identity crimes, it is still easy for a criminal to take out loans in someone else's name, to run up enormous credit card debts and tap into bank accounts.

Numerical identifiers such as credit card numbers and social security numbers were originally designed to serve as means for verifying a person's identity. However, these numerical identifiers are easily obtained by a criminal. For example, a credit card receipt can be easily removed from a waste basket to obtain the credit card number. Social security numbers are often requested to be entered on all kinds of forms. Any person later coming into contact with such forms can easily obtain the social security number.

Various technologies have been devised in attempts to solve the problem of identity crimes. For example, biometrics such as fingerprint recognition equipment can be used to determine or confirm a person's identity by scanning the person's fingerprint and comparing it to an earlier stored fingerprint of the person. Retinal scans or DNA analysis can also be used to identify a person. Such equipment is very expensive to replicate on a large scale.

Banks often use a personal identification number (PIN) to verify the identity of a person. A bank customer is required to enter his or her PIN prior to withdrawing cash from his or her account. This PIN is a static number (i.e., it does not change for each transaction) and it can be reused over and over again. Therefore, there is a risk that a criminal can obtain a PIN number from a previous transaction and simply reuse it to perpetrate a crime. In other words a PIN number must be kept hidden even after it is used. Furthermore, PIN's are specific to a single account and are not used universally to all types of transactions in a person's life.

Another example of a situation in which verifying a person's identity is important is in preventing children from entering adult only orientated establishments, For example, bars and nightclubs often need to determine the age of a patron to ensure that the patron is not a minor. Typically these establishments use a patron's driver's license to ascertain their age. However, minors often obtain fraudulent drivers licenses by inserting their photograph into a stolen or otherwise obtained driver's license of an adult. Similar methods may be used to falsely assert an older age for purchasing cigarettes or alcohol. Use of fingerprint or other recognition equipment is typically too expensive for these establishments and therefore enforcement of the laws is difficult.

The recent advances in commercial transactions over the Internet have also created an interest by purchasers in verifying the identity of the entity they are doing business with. Before providing a credit card number to purchase an item or transact some form of business, the person desires to gain some assurance that the entity with whom they are transacting the business is reputable.

Summary of the Invention

An identity verification method is provided. The identity verification method includes the steps of obtaining a list of at least two identity verifiers and linking the identity verifiers to at least one numerical identifier wherein the numerical identifier is associated with a registered user. The method also includes the steps of receiving a numerical identifier and an identity verifier from a requesting party and determining whether the received identity verifier is linked to the received numerical identifier. The method includes communicating information to the requesting party indicating whether the received identity verifier is linked to the received numerical identifier.

In accordance with another aspect of the invention, a method of determining whether an identity verifier is required to be submitted in a particular transaction is also provided.

In accordance with another aspect of the invention, an identity verification system is provided. The system includes a database, an input module, a communications module and a processor module.

In accordance with another aspect of the invention, a remote terminal for communicating with an identity verification system is provided. The remote terminal includes an input module and a communications module.

In accordance with another aspect of the invention, a computer program storage medium readable by a computing system and encoding a computer program of instructions for executing a computer process is provided. The computer process stores at least two identity verifiers in a database. The computer process also stores at least one numerical identifier associated in a database wherein the numerical identifier is linked to the at least two identity verifiers. The computer process receives a numerical identifier and an identity verifier. The computer process compares the received numerical identifier and the received identity verifier to the stored numerical identifiers and identity verifiers to determine whether the received identity verifier is linked to the received numerical identifier. The computer process also communicates information indicating whether the received identity verifier is linked to the received numerical identifier.

Brief Description of the Drawings

Figure 1 illustrates one embodiment of an identity verification system in accordance with the principles of the present invention.

Figure 2 illustrates one embodiment of an identity verification system in accordance with the principles of the present invention.

Figure 3 illustrates one embodiment of a computer system in accordance with the principles of the present invention.

Figures 4a-4c are a flow chart diagram of one embodiment of a method of verifying the identity of a registered user in accordance with the principles of the present invention.

Figure 5 illustrates one preferred method of creating lists of identification verifiers in accordance with the principles of the present invention.

Figure 6 illustrates one portion of a registered users record according to one preferred embodiment of the present invention.

Figure 7 is an exemplary index for locating a registered user's record based on a numerical identifier in accordance with the principles of the present invention.

Figure 8 is an exemplary table of records and associated pointers in accordance with the principles of the present invention.

Figure 9 is an exemplary table of transactions associated with pointer number 96804294 of the first record in Figure 8 in accordance with the principles of the present invention.

Figure 10 is an exemplary table of identity verifiers associated with pointer 34682141 of the first record in Figure 8 in accordance with the principles of the present invention.

Detailed Description of the Invention

The methodology of the present invention can be implemented in many different ways. These different ways do not require use of a computer system. However, in one preferred embodiment a computer system is used to implement the methodology of the present invention. Therefore, this detailed description begins with a description of one embodiment of a computer system implementation of the invention.

Figure 1 illustrates one embodiment of a computer system in accordance with the present invention. The remote terminal 200 communicates through a communications network 158 with a server computer 100. An input module 206 is connected to the server computer 102.

A remote terminal is a communications device that is capable of sending and receiving information through a communications network. Remote terminal 200 includes an output module 201, an input module 202, and a communications module 204.

Some preferred embodiments of remote terminal 200 are illustrated in Figure 2. One preferred embodiment of remote terminal 200 is a magnetic card swipe and keypad device 156 having a keypad 125, magnetic card reader 127 and output display 131. Another preferred embodiment of remote terminal 200 is a telephone 156'. Alternatively, remote terminal 200 could be a computer 156" including keyboard 145 and monitor 147.

Returning to Figure 1, input module 202 is capable of inputting information into the remote terminal 200. In a preferred embodiment shown in Figure 2, input module 202 is a keypad 125, a card swipe reader 127, or both. In another preferred embodiment, the input module 202 is a keyboard 145 connected to a computer 156". In another preferred embodiment, the input module is a receiver 151 on telephone 156'.

Communications module 204 of the remote terminal 200 is capable of receiving and transmitting information to and from communications network 158. In a preferred embodiment, communications module 204 is a modem or other communications hardware as typically used on a credit card reading device. Alternatively, the communications module 204 can simply be the components of a telephone that allow communications over a telephone line.

In a preferred embodiment of the invention, output module 201 is a display screen 131. In another preferred embodiment, the output module 201 is a monitor 147. In another preferred embodiment, the output module 201 is a transmitter in a telephone.

Computer 100 includes a processing module 212 connected to a database 210 and also connected to a communications module 214. It is important to note that even though the database 210 is shown as being in the computer 100, the memory in which the database resides could alternatively be offsite from the computer 100.

A processing module is a module capable of executing a series of instructions in a program and it includes a central processing unit (cpu) such as a microprocessor.

Figure 2 illustrates a possible organization for a computing system for implementing an embodiment of the present invention. The computing system includes a plurality of devices connected together using communications network 158.

The devices of the computing system include remote terminals that may include card swipe and keypad device 156, telephone 156' and client computer 156". Other types of remote terminals may be utilized. The computing system also includes server computer 102 having monitor 152, keyboard 144 and mouse input device 146. The computer 102 in this embodiment is connected to the communications network 158 for communicating with the remote terminals 156, 156' and 156".

Remote terminals 156 include a keypad 125 for inputting information, and a magnetic card swipe reader 127 also for inputting information.

The server computer 102 receives service requests from the remote terminals 156, 156' and/or 156", as will be described below, and generates appropriate responses.

The communications network 158 of a preferred embodiment is a wide area network (WAN). In one possible embodiment of the invention, the WAN may be the Internet in which user computers 156" are connected using a typical dial-up connection through an internet service provider (ISP).

In another preferred embodiment the communications network 158 may be a local area network (LAN).

In yet another preferred embodiment, the communications network 158 could be simply a telephone line connecting telephone 156' to telephone 157. In this preferred embodiment, the telephone 157 is situated near an input device such as keyboard 144 and mouse 146 so that a person can interface between voice communications via telephone 157 and the computer 102 to provide the necessary services to the person requesting such services from telephone 156'.

In another embodiment utilizing a telephone 156' as a remote terminal, an automatic telephone communication and messaging system may be used to provide automated communications between the person at telephone 156' and the computer 102 without intervention of another person at a telephone 157.

FIG. 3 illustrates computer 102 according to one embodiment of the present invention. An exemplary computing system for an embodiment of the invention includes a general purpose computing device in the form of a conventional computer system 102 including a processor unit 112, a system memory 114, and a system bus 116 that couples various system components including the system memory 114 to the processor unit 112. The system bus 116 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus and a local bus using any of a variety of bus architectures. The system memory includes read only memory (ROM) 118 and random access memory (RAM) 120. A basic input/output system 122 (BIOS), which contains basic routines that help transfer information between elements within the computer system 102, is stored in ROM 118.

The computer system 102 further includes a hard disk drive 123 for reading from and writing to a hard disk, a magnetic disk drive 124 for reading from or writing to a removable magnetic disk 126, and an optical disk drive 128 for reading from or writing to a removable optical disk 129 such as a CD ROM, DVD, or other optical media. The hard disk drive 123, magnetic disk drive 124, and optical disk drive 128 are connected to the system bus 116 by a hard disk drive interface 130, a magnetic disk drive interface 132, and an optical drive interface 134, respectively. The drives and their associated computer-readable media provide nonvolatile storage of computer readable instructions, data structures, programs, and other data for the computer system 102.

Although the exemplary environment described herein employs a hard disk, a removable magnetic disk 126, and a removable optical disk 129, other types of computer-readable media capable of storing data can be used in the exemplary system. Examples of these other types of computer-readable mediums that can be used in the exemplary operating environment include magnetic cassettes, flash memory cards, digital video disks, Bernoulli cartridges, random access memories (RAMs), and read only memories (ROMs).

A number of program modules may be stored on the hard disk, magnetic disk 126, optical disk 129, ROM 118 or RAM 120, including an operating system 136, one or more application programs 138, other program modules 140, such as a database management system, and program data 142. A user may enter commands and information into the computer system 102, through input devices such as a keyboard 144 and mouse 146 or other pointing device. Examples of other input devices may include a microphone, joystick, game pad, satellite dish, and scanner. These and other input devices are often connected to the processing unit 112 through a serial port interface 150 that is coupled to the system bus 116. Nevertheless, these input devices also may be connected by other interfaces, such as a parallel port, game port, or a universal serial bus (USB). A monitor 152 or other type of display device is also connected to the system bus 116 via an interface, such as a video adapter 154. In addition to the monitor 152, computer systems typically include other peripheral output devices (not shown), such as speakers and printers.

As discussed above with respect to Figure 1, a server computer 100, communicates through a communications network 158 with remote terminals 200. In the embodiment shown in Figure 3, the network connections include a local area network (LAN) 159 and a wide area network (WAN) 160. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets, and the Internet.

The computer system 102, is logically connected to one or more remote terminals, such as a remote terminal 155. The remote terminal 155 may be a computer system, a server, a router, a network PC, a peer device or other common network node, and as discussed above, may include a keypad and card swipe device 156 or a computer system 156".

When used in a LAN networking environment, the computer system 102 is connected to the communications network 158 through a network interface or adapter 162. When used in a WAN networking environment, the computer system 102 typically includes a modem 164 or other means for establishing communications over the wide area network 160, such as the Internet. The modem 164, which may be internal or external, is connected to the system bus 116 via the serial port interface 150. In a networked environment, program modules depicted relative to the computer system 102, or portions thereof, may be stored in the remote memory storage device. It will be appreciated that the network connections shown are exemplary, and other means of establishing a communications link between the computer 102 and the remote terminals 155 may be used.

A computing device, such as computer system 102 typically includes at least some form of computer-readable media. Computer readable media can be any available media that can be accessed by the computer system 102. By way of example, and not limitation, computer-readable media might comprise computer storage media and communication media.

Computer storage media includes volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules or other data. Computer storage media includes, but is not limited to, RAM, ROM, EPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium that can be used to store the desired information and that can be accessed by the computer system 102.

Communication media typically embodies computer-readable instructions, data structures, program modules or other data in a modulated data signal such as a carrier wave or other transport mechanism and includes any information delivery media. The term "modulated data signal" means a signal that has one or more of its characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media includes wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, RF, infrared, and other wireless media. Combinations of any of the above should also be included within the scope of computer-readable media. Computer-readable media may also be referred to as computer program product.

The logical operations of the various embodiments of the present invention are implemented (1) as a sequence of computer implemented acts or program modules running on a computing system and/or (2) as interconnected machine logic circuits or circuit modules within the computing system. The implementation is a matter of choice dependent on the performance requirements of the computing system implementing the invention. Accordingly, the logical operations making up the embodiments of the present invention described herein are referred to variously as operations, structural devices, acts or modules. It will be recognized by one skilled in the art that these operations, structural devices, acts and modules may be implemented in software, in firmware, in special purpose digital logic, and any combination thereof without deviating from the spirit and scope of the present invention as recited within the claims attached hereto.

A preferred method of verifying the identity of a registered user in accordance with the principles of this invention will now be explained with reference to the drawing figures.

A person or entity that applies for and is accepted into the identity verification method or system of the invention is referred to as a registered user. A registered user could be any individual who wishes to safeguard their identity or allow others to verify certain information about the registered user. A registered user could also be an entity such as an online retailer who utilizes the identity verification method or system of the invention to allow customers to obtain information about the retailer or to verify the identity of the retailer.

The identity verifier process may be used for checks (mailed, in person, over the Internet, over the telephone), credit card transactions (mailed, in person, over the Internet, over the telephone), loan applications, opening bank or credit card accounts, preventing phone slamming or cramming, carding patrons in bars, ensuring that adult only sites on the Internet are not visited by children, preventing Medicare fraud, authorizing automatic bill payments by check or credit card, and verification of identities without photographs.

The entity or entities implementing or running the identity verification method or system of the invention must take a preliminary step to set up a registered user. This step involves performing a background investigation of the potential registered user to make sure that the potential registered user is not attempting to use the identity verification method to further perpetrate a crime. This investigation should focus on ensuring that the identity of the potential registered user is as presented by the potential registered user.

It is envisioned that the entity managing the identity verification system would have agents located throughout the market place (e.g., at banks throughout the country) to implement the registration of a user.

Turning now to Figure 4a, the generate operation 400 involves obtaining or generating a list of identification verifiers (idv's). An identification verifier is any n-digit string of random characters, symbols or numbers. For example an identification verifier could be a five digit number like 83604 or 01781. Alternatively, an identification verifier could be a six digit combination of characters, symbols and numbers such as B#1?C%.

The number of characters or digits in an idv depends on the number of transactions the particular registered user will be engaged in. For example, a user with a small number of transactions may have a list of 200 idv's each of which is 5 digits long such as any numbers between 00000 and 99999. Alternatively, a government agency which writes many checks may have 200,000,000 idv's, each of which is 11 digits long such as numbers between 00000000000 and 99999999999.

Idv's can be obtained or generated in many different ways. It is important to generate the idv's in such a way as to minimize the possibility of reverse engineering lists of idv's. Reverse engineering of idv's would, for example, allow someone to determine the nature of the next idv on a list of idv's by knowing earlier idv's and understanding the algorithm used to generate the idv's.

A list of random numbers that is comprised of mixed true and pseudo-random numbers cannot be reverse engineered. A pseudo random number is created by a computer program called a random number generator. It is not technically random because running the program with the same initial seed number will always produce the same list of random numbers. Generating such a table is even easier if the numbers do not need to be equally distributed, which is the case for this invention. If several idv lists are being created at the same time, and several methods of generating numbers are interspersed, reverse engineering of the numbers in the lists becomes impossible.

Figure 5 illustrates a preferred embodiment of the generate operation 400. Two random number generating algorithms A and B as well as a true random number generating method based on a clock time are used in an interspersing manner to create lists of idv's that cannot be reverse engineered. As can be seen in Figure 5, algorithm A generates and places the first idv in each of five idv lists beginning with list 1 and ending with list 5. Algorithm B generates and places the second idv in each of the five idv lists beginning with list 1 and ending with list 5. Algorithm A then generates and places the third idv's in the five lists beginning with list 5 and ending with list 1. Algorithm B then generates and places the fourth idv's in the five lists beginning with the list 5 and ending with list 1. Then the true random generator based on clock time generates and places the fifth idv's in the five lists beginning with list 1 and ending with list 5. This process can be repeated as many times as is necessary. Alternatively the order of algorithms can be altered instead of repeated. As can be seen there are a large number of variations of the above process of creating or generating a list of idv's and this is but one example.

In a preferred embodiment of the methodology of the invention, the idv list is massaged to eliminate the problem of any random number repeating itself too soon in the list. In other words, a number or string of characters used for an idv may be repeated as an idv later in time. However, a "relevant range" must be defined to make sure that the same number or string of characters is not used too close in a list to each other. For example, a relevant range could be defined as 60 days. This means the method for generating idv's must ensure that in a 60 day period, assuming an average number of transactions, no two idv's will be the same. Modifying the size of the replenishment list (later list) can enforce this constraint.

It is also within the scope of the methodology of this invention for the idv lists to be obtained from an entity other than the entity that owns or runs the identity verification system. For example the idv lists could be generated off site from the server computer 100 and downloaded or otherwise inputted into the database 210.

Once the idv list is generated, it is given to the registered user. The registered user can store the list of idv's on a password protected electronic calculator-like memory device which functions as a storage and access device for the list. Alternatively, the list can be stored on paper.

The list of idv's does not have to be used sequentially by the registered user. However, only idv's within the relevant range should be used. This characteristic permits a user to use the system without concern about absolute order of use of the list of idv's. For example, the user can write and mail a check that includes an idv that will be used after another transaction performed later in the day.

Note also that if a registered user loses its list of idv's, a new list would be generated. This new list would contain entirely new idv's not on the lost list.

The create categories operation 401 sets up categories of requesting parties so that the registered user can differentiate the information to be supplied to each category. Some example categories are: bank, retailer, tavern, phone company, purchaser, car dealer, etc. These categories may be preset prior to registration of a user or they may be created by the user at the time of registration.

The receiving public information operation 402 involves obtaining certain information about a registered user or prospective registered user. In a preferred embodiment of the invention, the information is stored in a record associated with the registered user, the record residing in the database 210.

In a preferred embodiment the registered user decides which information will be supplied to the record. Examples of information that could be provided are age, name, middle name, phone numbers, date of birth, social security number, drivers license number, credit card numbers, banking account numbers. In a preferred embodiment at least one existing numerical identifier is received into the record. It is noted that this information including changes in numerical identifiers should be updated from time to time as may be necessary.

A numerical identifier is any code, number or symbol typically associated with a particular person but that could be associated with more than one person. Examples, of numerical identifiers are social security number, drivers license number, credit card numbers, banking account numbers (as long as the routing number is included), phone numbers, etc.

Some of these numerical identifiers are shared between two or more people. For example, a couple sharing a checking account results in both individuals being associated with the same numerical identifier (the checking account number). These shared numerical identifiers can be made unique to a particular person by assigning a suffix to the shared numerical identifier. For example, the husband in the above example could be assigned suffix 1 such as a number 01, and the wife could be assigned suffix 2, such as number 02. By including the suffix with the original numerical identifier, a made unique numerical identifier is created.

Further information that is preferably obtained in the receiving public information operation 402 includes information about which transactions will not be covered by the identity verifier process. For example, a registered user may decide that checks under $20 from a specific checking account will not require an idv. As another example, a registered user may indicate that use of a particular credit card will not require an idv while all other transactions will require an idv.

Assigning suffix operation 403 determines whether a uniqueness suffix is required, and if so, assigns a suffix. This suffix may be stored in the uniqueness suffix column as shown in Figure 7.

A requesting party is any party attempting to verify the identity of a person through the identity verification process. Examples of requesting parties are banks, retailers, credit card companies, nightclubs, online retailers, online shoppers, etc.

The receive information operation 406 involves obtaining instructions from the registered user indicating which public information (e.g., age, name, middle name, home phone number, work phone number, other phone numbers, date of birth, social security number, driver license number) to make available to which categories of requesting parties.

Figure 6 is an example partial record stored in the database 210 and associated with a particular registered user. The right most column of the record in Figure 6 contains personal information about the registered user. The left columns each represent a particular category of requesting party such as bank, retailer, tavern, phone company, purchaser, car dealer, etc. There is also a miscellaneous catch all column entitled "other". For each of these left columns, a check mark is placed in the rows for which the indicated information can be released. So, for example, if the requesting party is a tavern, then the only information that can be provided to the requesting party is the age of the registered user. On the other hand, this particular registered user has indicated in Figure 6 that if the requesting party is a bank, then the name, work phone, address, city, state, zip, social security number and middle name may be provided to the requesting party.

By indicating which information is to be provided to a particular category of requesting party, the method of invention allows release of information necessary for a particular transaction while protecting all other information about the registered user.

In the interest of privacy, the requesting parties that fit within the categories that allow for the release of larger amounts of information may be required to submit a password or a special idv list to prove that they are truly in such a category.

A preferred embodiment of this process would require that any party wishing to obtain such a password to submit themselves to a background investigation to prove the identity of such a requesting party and/or to determine the trustworthiness of such a party. Once such a successful investigation is completed, the requesting party would be provided with a password. Once armed with a password or special idv list, this requesting party could submit the password to the entity running the identity verification process to prove its category and therefore obtain higher levels of information about the registered user.

Linking idv's operation 408 of Figure 4a links the list of idv's from the generating operation 400 to the registered party's record. This record is preferably stored in a database 210. Figure 8 illustrates three example rows of entries in a database 210. Each row represents a single registered user's record. The first column is entitled "relative record number" and the numbers in this column are numbers that identify the record. The second column is entitled "list of transactions that require an idv". The second column contains a number or pointer that points to another portion of the record devoted to listing the transactions for which the registered user has indicated are to require an idv. For example, the first row of the second column points to the portion of the record illustrated in Figure 9.

Figure 9 provides an example record portion for identifying the transactions that require an idv. In this example, all financial transactions require an idv except the items listed in the fourth row.

The third column in Figure 8 contains a number that points to the record portion that contains the table of idv's. In one preferred embodiment, this pointer is the way in which the list of idv's is linked to the registered user's record. An exemplary table of idv's is illustrated in Figure 10.

The list of idv's is placed in the first column of the table in Figure 10. For example, the number "68231" is a five digit idv. The second column contains the corresponding verification transaction identifier that will be explained more fully below.

The third column contains space for storing time and date information about the transaction. This time and date information basically is the time and date of the transaction which can be recorded in many different ways including by the remote terminal or by the computer system or by a human operator of the system who manually enters the time and date.

The fourth column contains space for storing information about the requesting party. This fourth column can contain communication origin information. Communication origin information is some code for identifying the requesting party. For example, the communication origin information could the phone number, Internet address, fax number, or email address of the requesting party. In a preferred embodiment, this communication origin information is received by the server computer 100 at the time of receipt of the numerical identifier.

The fifth column provides space for storing optional information such as a message about the transaction such as the amount spent and the payment method.

As will be described in more detail below, the message in the 5th column of Figure 10 is provided as an extra security measure for certain transactions. This message can be entered into the system by the registered user prior to completion of a transaction. Then, when the transaction is completed, another interested party can compare the information in the 5th column with the information received from the transaction. The information in the 5th column may alternatively be stored in the optional database.

An example of a use of the optional database or 5th column message of Figure 10 is now provided. Suppose a person's checks are being stolen from mailboxes. The idv's on the checks can be used by check counterfeiters. To overcome this, a person can supply pertinent details associated with the idv to the system. For a check, the registered user may send (via Internet or voicemail converted to text via speech recognition software) the idv, the check's recipient, the amount, the date, and even the recipient's address to the optional information portion of the record (e.g., 5th column of Figure 10) after supplying one of the registered user's unique numerical identifiers and a password. The recipient of a counterfeit check containing a valid identity verifier then will be provided details and, seeing the inconsistency, will be alerted that fraud is being attempted.

The optional database (i.e. the optional 5th column of Figure 10) may be used to help protect government agencies from check fraud and counterfeiting. For example, the government agency may want to ensure that Medicare checks are cashed only by the person specified and only for the amount specified on the check. In such an example, the optional information associated with the check's idv (the information that would be stored in the 5th column of the record shown in Figure 10) could state the amount of the check and the recipient's social security number. When the recipient of the government check cashes the check they must submit their own idv. The identity verification process of this invention then uses the recipient's social security number and idv to verify the identity of the recipient before cashing the check.

In the government check example, the idv is present on the face of the check. The check number could also serve as the government's idv for the check. Because the process in this example is utilizing the optional information, the transaction is still secure despite the ability to guess or determine the idv's on the checks.

It is noted that the information in the table of Figure 10 is saved and archived for legal and audit purposes. The information stored in the table of Figure 10 can be valuable to track a parties' financial or other transactions. Furthermore, such information may be valuable to resolve a legal dispute about a particular transaction. For example, some events, like will signings, will be verified years after an event's date.

Returning to Figure 8, the fourth column contains a number that points to the public information table of Figure 6, which was already described above.

Figure 7 illustrates a list of numerical identifiers that may be preferably stored in database 210. The list of numerical identifiers provides pointers to the record of the associated registered user. In other words, the table of Figure 7 is an index that allows an inputted numerical identifier to be used to locate the corresponding registered user's record.

The first column of the index of Figure 7 contains the numerical identifier type. For example a type of "0" could represent social security numbers, a type of "1" could represent drivers license numbers, and a type of "2" could represent credit card numbers. The second column lists the numerical identifiers. The third column lists any optional uniqueness suffix. The fourth column contains a pointer to the registered user's record. Note that a registered user can have multiple numerical identifiers in the database. Therefore, the same record number can be associated with different numerical identifiers.

Returning to the operations of Figures 4a-c, once the idv list is linked to the registered user's record, the system is ready to be utilized in a transaction. The registered user armed with its list of idv's (obtained from the system in operation 409) initiates a transaction by providing the requesting party with a numerical identifier and an unused idv from the registered user's list of idv's. The requesting party then submits the numerical identifier and the idv to the identity verifier system of this invention. As discussed earlier, the submission of the numerical identifier and the idv to the system can be done in many different ways including but not limited to by telephone, over the Internet, or via an electronic remote terminal similar to a credit card reader.

Receiving information operation 410 involves obtaining information from the requesting party. The information received should include at least one numerical identifier. Any numerical identifier registered with the system may be used. The information received may also include an idv and other information. The operation 410 can be performed by receipt of a phone call and obtaining the numerical identifier via voice communications. Alternatively, the operation 410 can be accomplished by electronic transfer of the information over a communications network such as a WAN or LAN.

Determining operation 412 involves comparing the numerical identifier received in operation 410 with a general list of numerical identifiers of all registered users to see if the received numerical identifier is present on the general list. In a preferred embodiment, the general list is stored in the database 210 as a table such as illustrated in Figure 7.

If the result of the determining operation 412 is that the numerical identifier received in opertion 410 is not present in the database, then operation flows to communication operation 414. Communication operation 414 sends a message to the requesting party indicating that the party attempting to be identified in the transaction is not registered.

If the result of the determining operation 412 is positive, that is, the numerical identifier is in the database, then operation flows to the suffix determining operation 416. Suffix determining operation 416 performs a review of the general list of numerical identifiers (such as the exemplary list shown in Figure 7) to ascertain whether the numerical identifier received requires a uniqueness suffix. If a uniqueness suffix is required, then the suffix determining operation 416 determines whether a suffix has been received.

If a uniqueness suffix is required and one was not provided, then the operation flows to communication operation 418. Communication operation 418 sends a message to the requesting party indicating that an identity crime is potentially being attempted.

If a uniqueness suffix is not required or is correctly received, then operation flows to locating record operation 420. Locating record operation 420 identifies the registered user's record based on the numerical identifier (and if required the uniqueness suffix).

Determining operation 422 reviews the information received in receiving information operation 410 and searches for an idv. If an idv is not received, then operation flows to determining operation 424.

Determining operation 424 reviews the registered user's record to determine whether the particular transaction being considered is on the list of transactions that require an idv. An example of such a list was discussed above in reference to Figure 9. If an idv is required, then communication operation 430 sends a message to the requesting party indicating that an idv is required and that an identity crime is potentially being attempted. If an idv is not required for the type of transaction being entered into, then the communications operation 428 sends a message to the requesting party indicating that an idv is not required for this particular transaction.

If an idv was received in receiving operation 410, then operation flows from operation 422 to determining operation 432. Determining operation 432 compares the received idv with the list of idv's in registered user's record to determine whether the received idv is within the relevant range of registered user's list of idv's. In other words, the determining operation 432 only searches idv's within the relevant range. Implementation of the comparison may be accelerated by prior creation of a second sorted copy of the list if idv's with pointers to the location of each idv in the original list.

If the idv received is not within the acceptable range of registered user's idv's, then communication operation 434 sends a message to the requesting party indicating that an identity crime is potentially being committed.

If the idv received is within the acceptable range of registered user's idv's, then determining operation 436 compares the received idv with a list of idv's already used to determine whether the received idv has been used before.

As discussed above, idv character strings may be repeated as long as the repeat occurs outside a "relevant range". Therefore, the search in operation 436 of previously used idv's should only search within the relevant range of the idv list.

If the received idv has been used before, then communications operation 438 sends a message to the requesting party indicating that the submitted idv has already been used before. There are two main possible reasons that an idv would have already been used. First, the second attempt to use the idv could be an identity fraud attempt. Second, the type of transaction being performed might have two legitimate requesting parties. For example, in a payment by check type of transaction, the registered user may write out a check to a retailer and provide an idv to the retailer. The retailer submits the idv to the identity verification system and obtains verification of the registered user's identity (and receives a verification transaction identifier). The retailer then attempts to cash the check at a bank. The bank may submit the idv to the identity verification system. This submission would be a second use of the idv, but it would not be an attempted identity crime. The flow operations 438, 440, 441, 442 and 443 distinguishe between these two possible reasons for multiple idv use. Communications operation 438 requests submission of an earlier verification transaction identifier.

Communications operation 438 may receive an earlier verification transaction identifier from the requesting party in response to the request.

Determining operation 440 determines whether a verification transaction identifier is provided. If no verification transaction identifier is provided, then communicating operation 442 sends a message to the requesting party indicating that an identity crime is potentially being attempted.

Determining operation 441 compares the verification transaction identifier received in operation 438 with the verification transaction identifier linked to the already used idv. If the two verification transaction identifiers are the same, then communication operation 443 sends a message to the requesting party that the transaction has already been verified and provides the time and date of the initial verification as well as any other necessary information. If the comparison performed by determining operation 441 is negative, that is, the verification transaction identifiers are not the same, then operation flows to communications operation 442.

Returning to determining operation 436, if the idv has not been used before, (within the relevant range) then operation flows to determining operation 444.

As discussed above, it is often desired to associate some information or message with an idv to provide another level of fraud protection. Determining operation 444 reviews the registered user's record to determine whether the received idv is associated with a message. In the example record provided in Figure 10, the associated message is provided in the 5th column of the table.

If a message is associated with the idv, then communicating operation 446 sends the message associated with the idv to the requesting party. At this point the requesting party can compare the message received from the system to the information received by the party providing the idv. If the message received from the system is not the same and the information from the party providing the idv, then the requesting party can reasonably determine that fraud is being attempted and can therefore terminate the transaction.

Determining category operation 448 reviews information from the requesting party (received in the receiving operation 410) to and ascertains the category of the requesting party. This determining operation allows the system to eventually release only the pre-authorized information in the registered user's record to the requesting party.

Communicating operation 450 sends the verification transaction identifier associated with the idv to the requesting party. The requesting party may wish to save all verification transaction identifiers to prove that it verified the user's identity should the question be raised later by law enforcement or insurance investigators.

Communicating operation 450 also provides any pre-authorized information to the requesting party as is appropriate for the determined category of the requesting party as might be set forth in a record such as shown in Figure 6. For example, if the requesting party is a bar, and the registered user pre-authorized the category of bars to receive only age information, then only age information is provided to the requesting party.

Archiving operation 452 stores the information from the transaction such as the numerical identifier and all associated record information. This storage of information can be done in the database or on back of the tapes or by other means. Archiving operation 452 results in the ability to audit and prove past transactions.

Although the invention has been described in language specific to computer structural features, methodological acts and by computer readable media, it is to be understood that the invention defined in the appended claims is not necessarily limited to the specific structures, acts or media described. Therefore, the specific structural features, acts and mediums are disclosed as exemplary embodiments implementing the claimed invention.

The various embodiments described above are provided by way of illustration only and should not be construed to limit the invention. Those skilled in the art will readily recognize various modifications and changes that may be made to the present invention without following the example embodiments and applications illustrated and described herein, and without departing from the true spirit and scope of the present invention, which is set forth in the following claims.

Claims

WE CLAIM:

1. A method of verifying the identity of a registered user comprising the steps of:

(a) obtaining a list of at least two identity verifiers;

(b) linking the identity verifiers on the list to at least one numerical identifier wherein the numerical identifier is associated with the registered user;

(c) receiving a numerical identifier from a requesting party;

(d) receiving an identity verifier from a requesting party;

(e) determining whether the received identity verifier is linked to the received numerical identifier; and

(f) communicating information to the requesting party indicating whether the received identity verifier is linked to the received numerical identifier.

2. The method of claim 1 wherein the communicating information step signals that the received identity verifier is linked to the received numerical identifier by sending a verification transaction identifier to the requesting party.

3. The method of claim 1 further comprising the steps of:

(a) determining whether the identity verifier received from the requesting party has been used before; and

(b) communicating information to the requesting party signalling whether the identity verifier has been used before.

4. The method of claim 2 further comprising the step of archiving the identity verifier and the verification transaction identifier.

5. The method of claim 1 further comprising the steps of:

(a) storing public information about the registered user whose identity is to be verified;

(b) creating at least two categories of requesting parties;

(c) receiving instructions from the registered user regarding what public information is allowed to be released to each of the at least two categories of requesting party;

(d) determining the category of the requesting party;

(e) communicating the appropriate public information to the requesting party pursuant to the instructions from the registered user.

6. The method of claim 1 wherein the at least one numerical identifier is a social security number.

7. The method of claim 1 wherein the at least one numerical identifier is a drivers license number.

8. The method of claim 1 wherein the at least one numerical identifier is a bank account number.

9. The method of claim 1 wherein the at least one numerical identifier is a phone number.

10. The method of claim 1 wherein the at least one numerical identifier is a credit card number.

11. The method of claim 1 further compromising receiving a uniqueness suffix and wherein the determining step comprises determining whether the received identity verifier is linked to the received numerical identifier and the received uniqueness suffix.

12. The method of claim 1 wherein the steps of receiving a numerical identifier, receiving an identity verifier and communicating information to the requesting party are performed by voice communications over a phone line.

13. The method of claim 1 wherein the steps of receiving a numerical identifier, receiving an identity verifier and communicating information to the requesting party are performed through electronic communication through a wide area network.

14. A method of determining whether an identity verifier is required to be submitted in a particular transaction comprising the steps of:

(a) obtaining a list of at least two identity verifiers;

(b) linking the list of identity verifiers to at least one numerical identifier wherein the numerical identifier is associated with a registered user;

(c) creating categories of transactions;

(d) receiving instructions from the registered user designating the categories of transactions that require an identity verifier;

(e) receiving a numerical identifier from a requesting party;

(f) receiving information from the requesting party specifying the type of transaction occurring;

(g) determining whether the transaction requires the use of an identity verifier; and

(h) communicating information to the requesting party wherein the information communicated indicates whether an identity verifier is required for the specified transaction.

15. An identity verification system for verifying the identity of a registered user, comprising:

(a) a database for storing information pertaining to a registered user, wherein the database is configured to receive at least one numerical identifier associated with the registered user and at least two identification verifiers associated with the registered user;

(b) an input module for inputting at least one numerical identifier associated with a registered user and at least two identification verifiers associated with a registered user into the database so that the at least one numerical identifier is linked to the at least two identification verifiers;

(c) a communications module for two way communications for receiving a numerical identifier and an identification verifier, and for communicating a message relating to whether the received numerical identifier is linked to the received identification verifier;

(d) a processor module for comparing the numerical identifier and identification verifier received by the communications module with the information in the database to determine whether the received numerical identifier is linked to the received identification verifier.

16. The identity verification system of claim 15 wherein the database and the processor module are contained within a single computer.

17. The identity verification system of claim 14 wherein the input module is a keyboard.

18. The identity verification system of claim 14 wherein the communications module is a serial port and a modem.

19. The identity verification system of claim 14 wherein the communications module is a network adapter.

20. A remote terminal for communicating with an identity verification system, the remote terminal comprising:

(a) an input module for inputting a numerical identifier and an identification verifier;

(b) a communications module for sending a numerical identifier and an identification verifier and for receiving a message indicating whether the numerical identifier is linked to the identification verifier.

(c) an output module for reporting the received message.

21. The remote terminal of claim 20 wherein the input module comprises a keypad.

22. The remote terminal of claim 20 wherein the input module comprises a keypad and a magnetic card reader wherein the magnetic card reader receives the numerical identifier and the keypad receives the identification verifier.

23. The remote terminal of claim 19 wherein the output module comprises a display screen.

24. The remote terminal of claim 19 wherein the output module comprises a monitor.

25. A computer program storage medium readable by a computing system and encoding a computer program of instructions for executing a computer process for verifying the identity of a registered user, the computer process comprising:

(a) storing at least two identity verifiers in a database;

(b) storing at least one numerical identifier associated with the registered user in a database, wherein the at least two identity verifiers are linked to the at least one numerical identifier;

(c) receiving a numerical identifier;

(d) receiving an identity verifier;

(e) comparing the received numerical identifier and received identity verifier to the stored numerical identifier and stored identity verifiers to determine whether the received identity verifier is linked to the received numerical identifier; and

(f) communicating information to the requesting party indicating whether the received identity verifier is linked to the received numerical identifier.

Abstract of the Invention

An identity verification method is provided. The identity verification method includes the steps of obtaining a list of at least two identity verifiers and linking the identity verifiers to at least one numerical identifier wherein the numerical identifier is associated with a registered user. The method also includes the steps of receiving a numerical identifier and an identity verifier from a requesting party and determining whether the received identity verifier is linked to the received numerical identifier. The method includes communicating information to the requesting party indicating whether the received identity verifier is linked to the received numerical identifier. A method of determining whether an identity verifier is required to be submitted in a particular transaction is also provided. An identity verification system is also provided. Furthermore, a remote terminal for communicating with the identity verification system is provided. In accordance with another aspect of the invention, a computer program storage medium readable by a computing system and encoding a program of instructions for executing a computer process is also provided.

FIG. 1

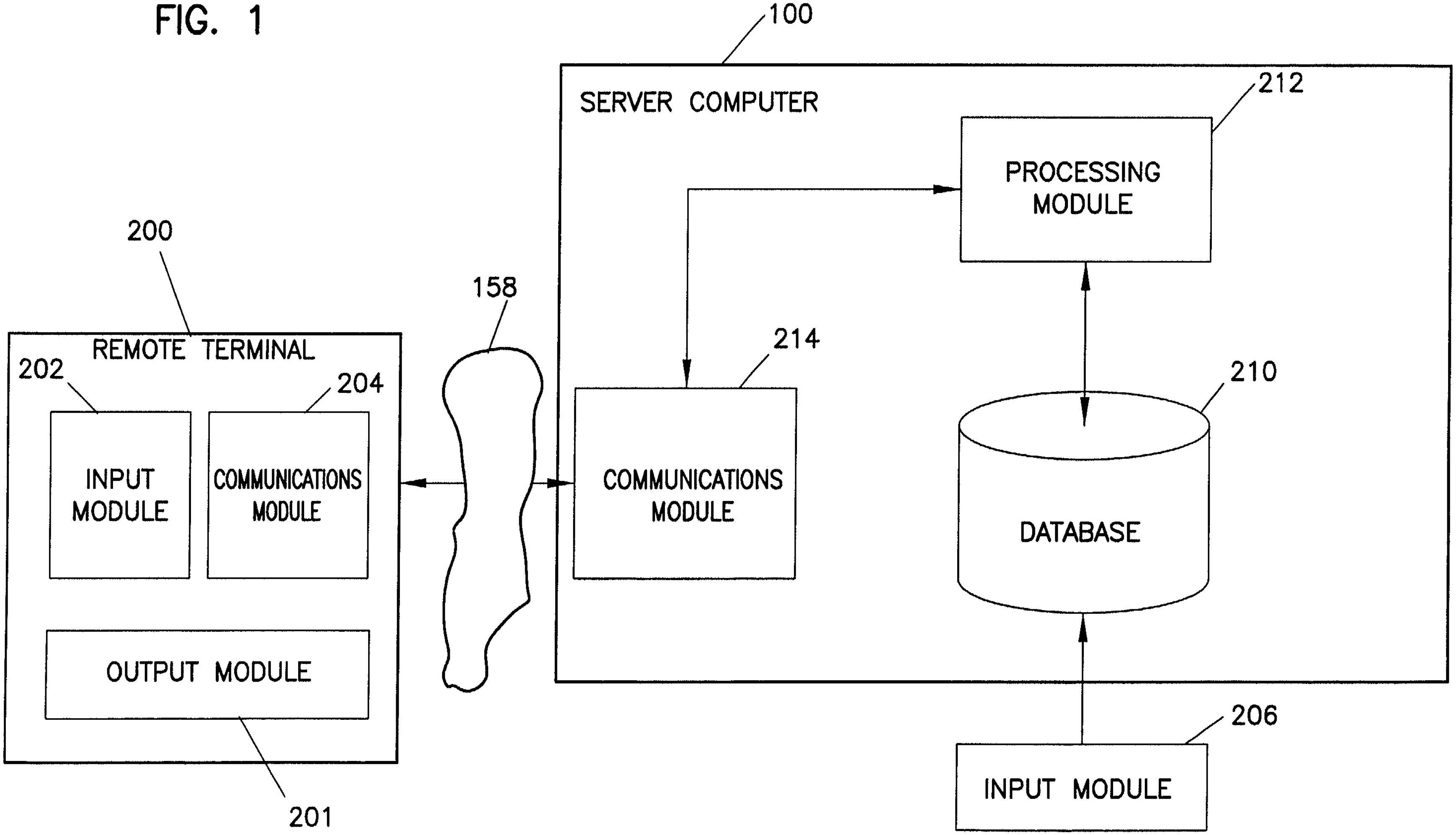
100
SERVER COMPUTER
212
PROCESSING MODULE
214
COMMUNICATIONS MODULE
210
DATABASE
206
INPUT MODULE
158
200
REMOTE TERMINAL
202
INPUT MODULE
204
COMMUNICATIONS MODULE
OUTPUT MODULE
201

FIG. 2

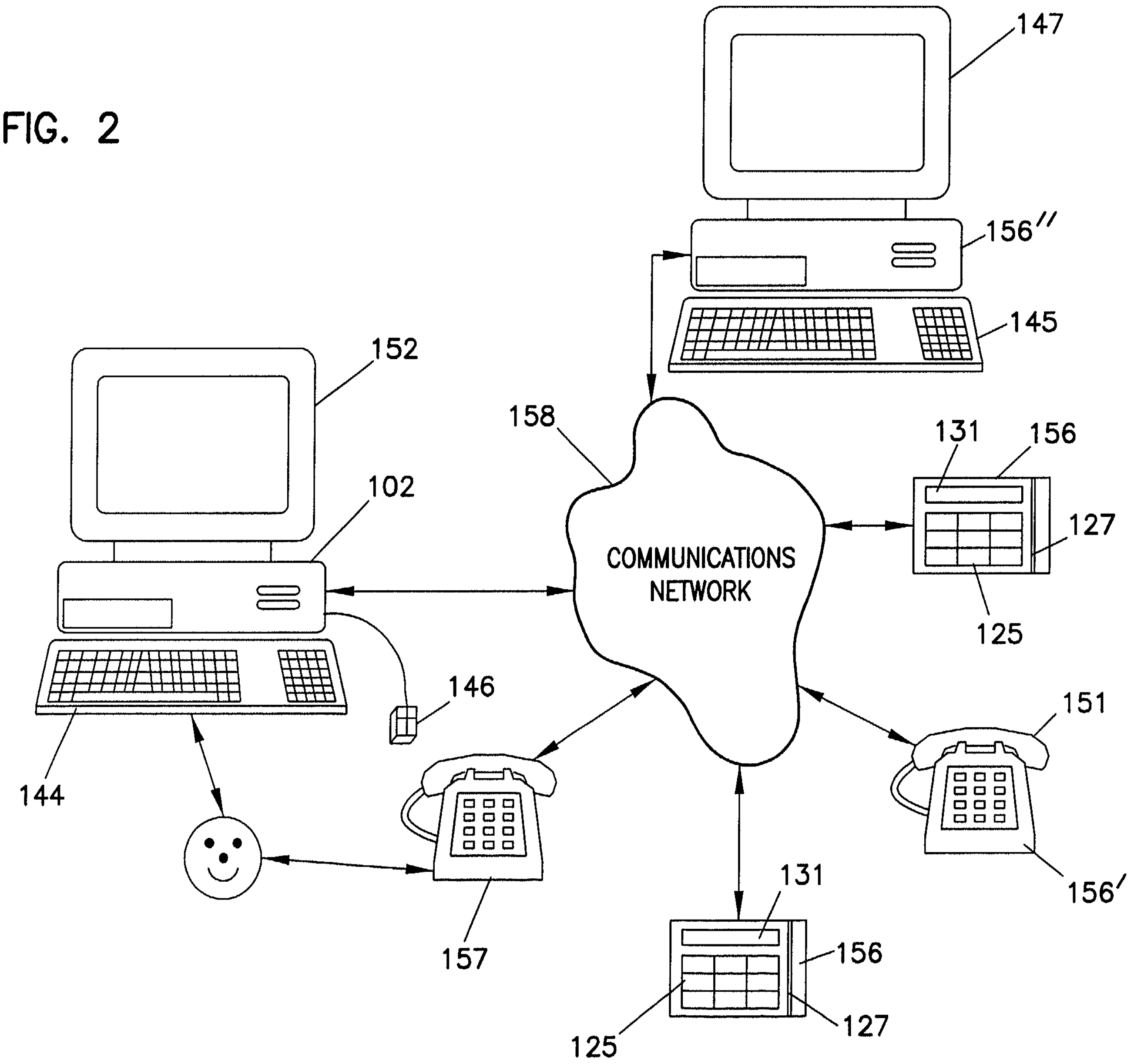
147
156″
145
152
102
158
COMMUNICATIONS NETWORK
131
156
127
125
146
144
151
156′
157
131
156
127
125

FIG. 3

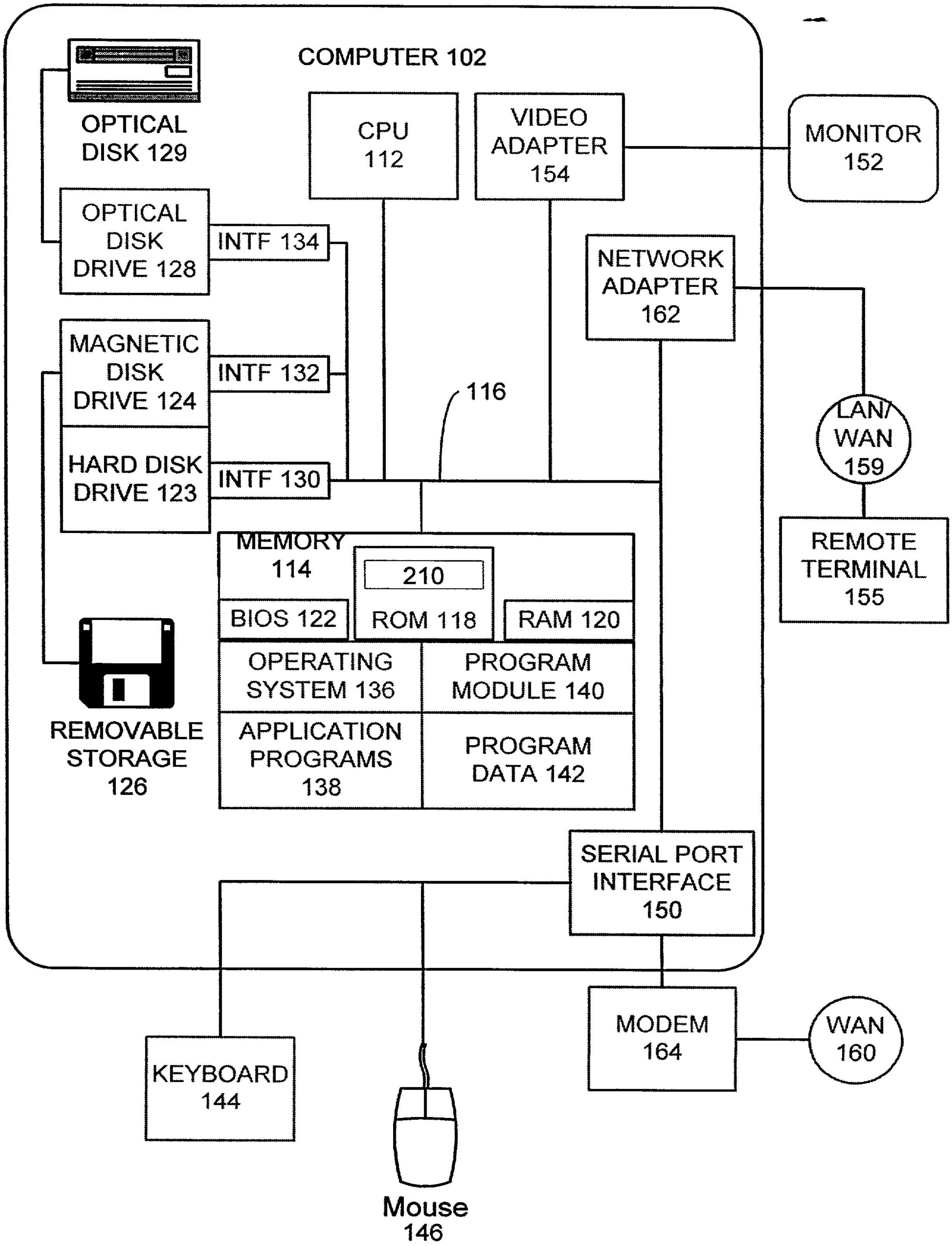
COMPUTER 102
OPTICAL DISK 129
OPTICAL DISK DRIVE 128
INTF 134
CPU 112
VIDEO ADAPTER 154
MONITOR 152
NETWORK ADAPTER 162
MAGNETIC DISK DRIVE 124
INTF 132
116
LAN/ WAN 159
HARD DISK DRIVE 123
INTF 130
REMOTE TERMINAL 155
MEMORY 114
210
BIOS 122
ROM 118
RAM 120
OPERATING SYSTEM 136
PROGRAM MODULE 140
APPLICATION PROGRAMS 138
PROGRAM DATA 142
REMOVABLE STORAGE 126
SERIAL PORT INTERFACE 150
MODEM 164
WAN 160
KEYBOARD 144
Mouse 146

FIGURE 4a

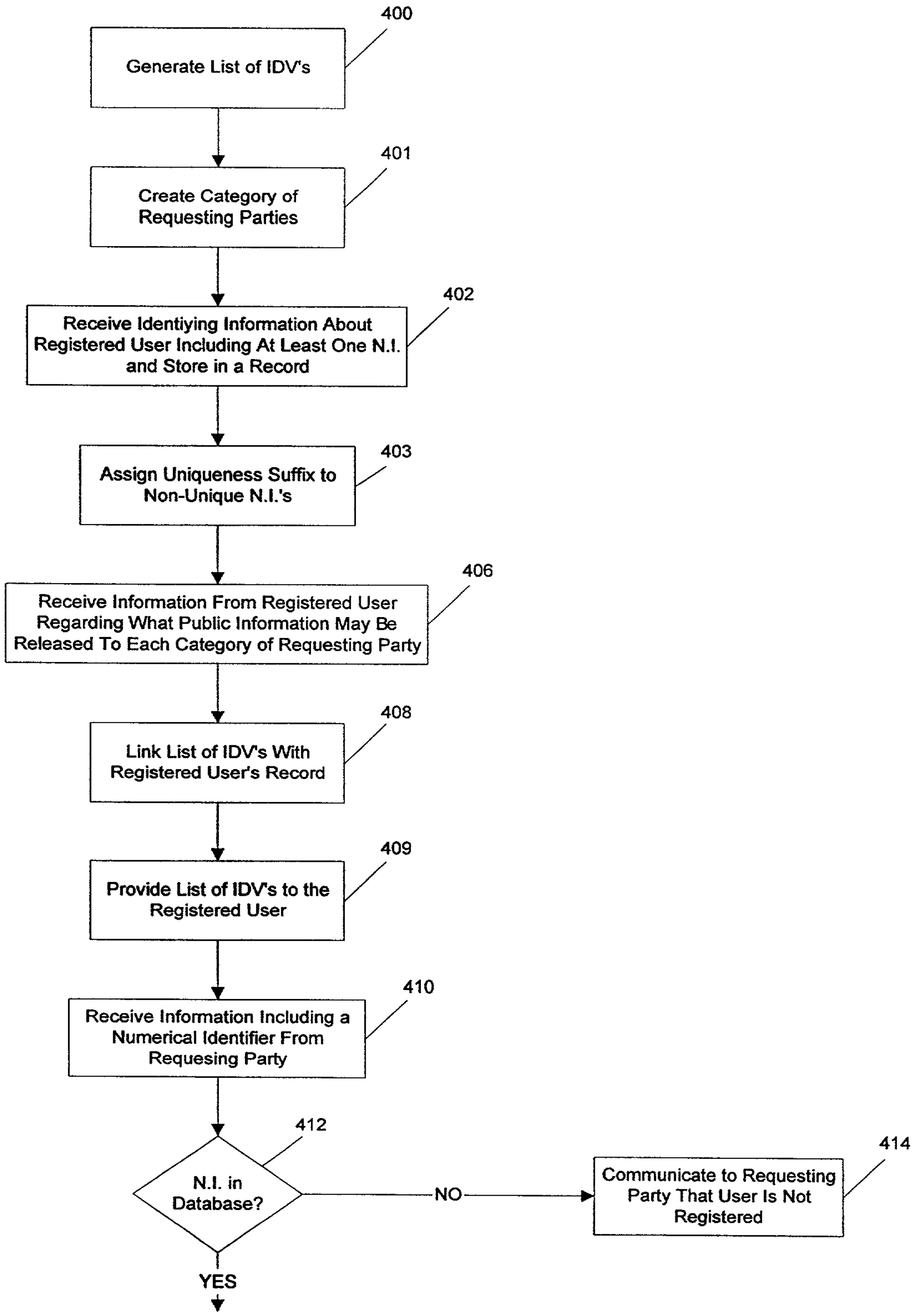
400
Generate List of IDV's
401
Create Category of Requesting Parties
402
Receive Identiying Information About Registered User Including At Least One N.I. and Store in a Record
403
Assign Uniqueness Suffix to Non-Unique N.I.'s
406
Receive Information From Registered User Regarding What Public Information May Be Released To Each Category of Requesting Party
408
Link List of IDV's With Registered User's Record
409
Provide List of IDV's to the Registered User
410
Receive Information Including a Numerical Identifier From Requesing Party
412
N.I. in Database?
NO
414
Communicate to Requesting Party That User Is Not Registered
YES

FIGURE 4b

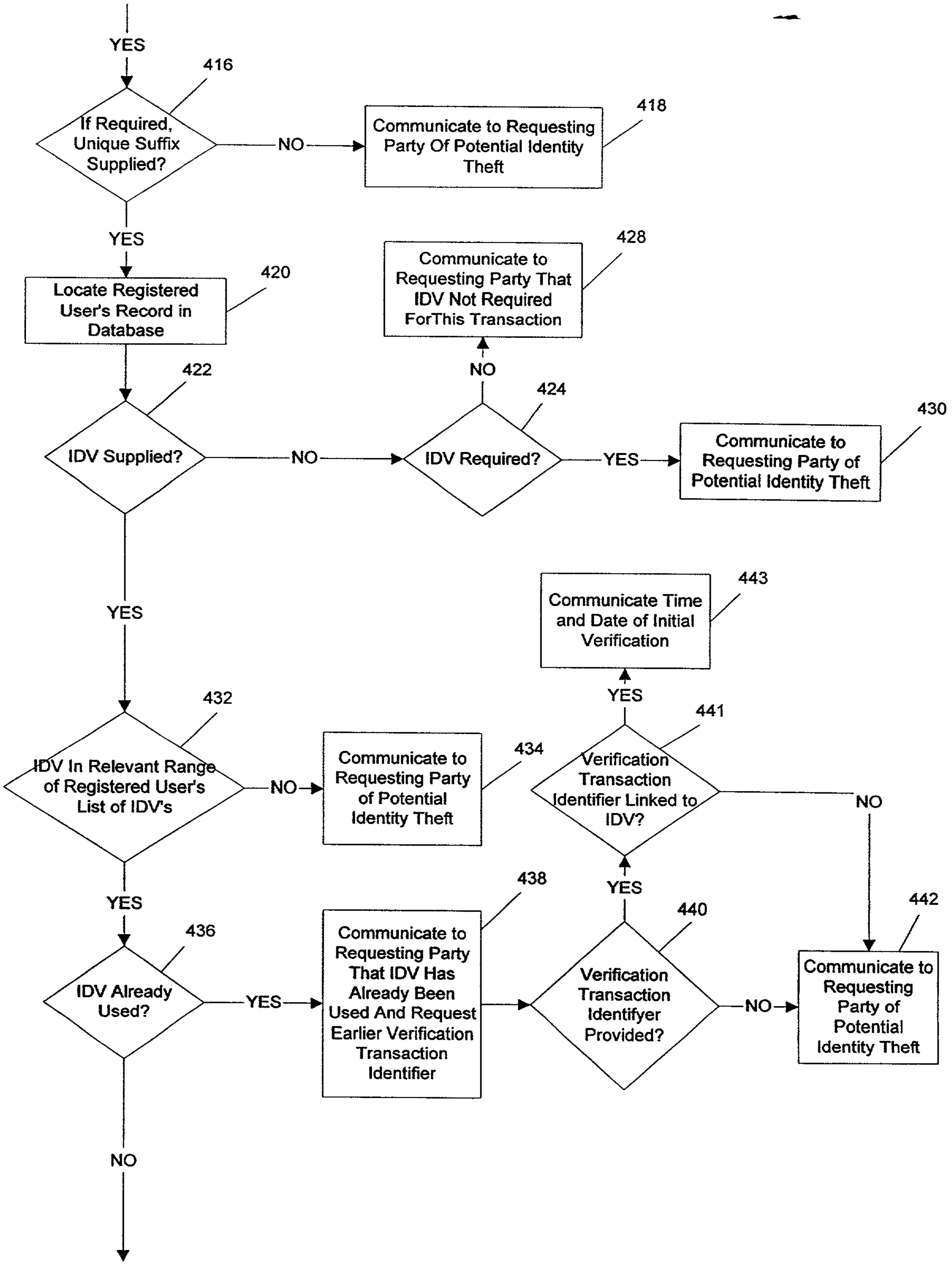
YES
416
If Required, Unique Suffix Supplied?
NO
418
Communicate to Requesting Party Of Potential Identity Theft
YES
420
Locate Registered User's Record in Database
428
Communicate to Requesting Party That IDV Not Required ForThis Transaction
NO
422
424
IDV Supplied?
NO
IDV Required?
YES
430
Communicate to Requesting Party of Potential Identity Theft
443
Communicate Time and Date of Initial Verification
YES
YES
432
441
IDV In Relevant Range of Registered User's List of IDV's
NO
434
Communicate to Requesting Party of Potential Identity Theft
Verification Transaction Identifier Linked to IDV?
NO
YES
438
YES
440
442
436
IDV Already Used?
YES
Communicate to Requesting Party That IDV Has Already Been Used And Request Earlier Verification Transaction Identifier
Verification Transaction Identifyer Provided?
NO
Communicate to Requesting Party of Potential Identity Theft
NO

FIGURE 4c

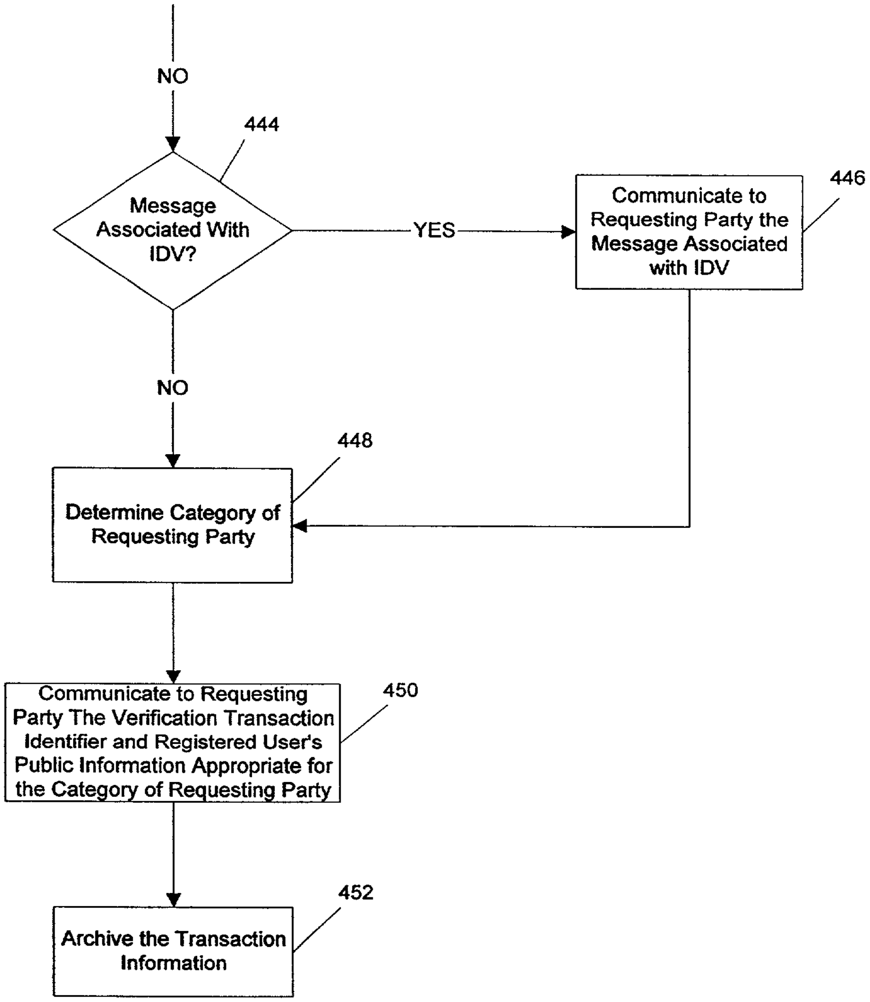
NO
444
Message Associated With IDV?
YES
Communicate to Requesting Party the Message Associated with IDV
446
NO
448
Determine Category of Requesting Party
Communicate to Requesting Party The Verification Transaction Identifier and Registered User's Public Information Appropriate for the Category of Requesting Party
450
452
Archive the Transaction Information

FIG. 5

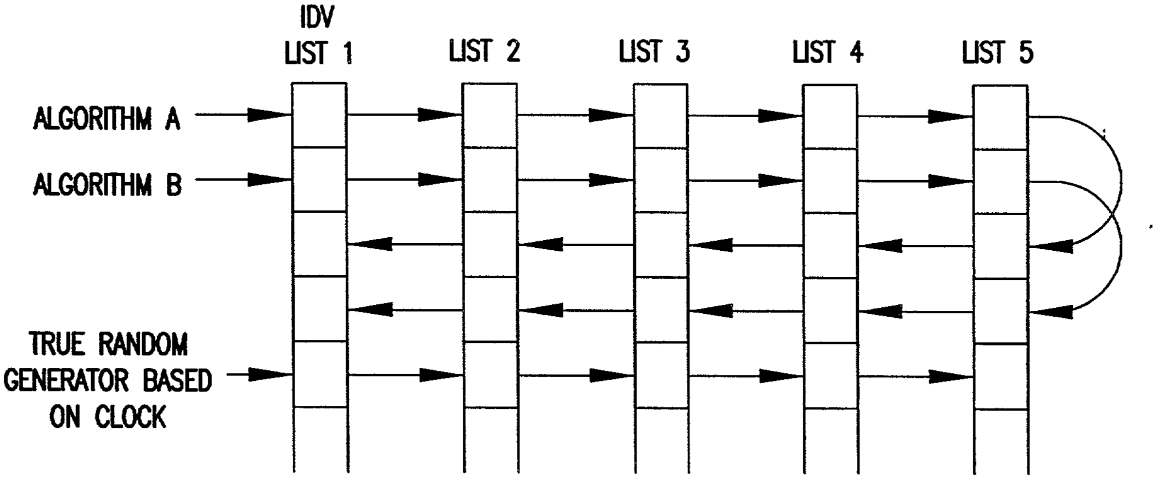
IDV
LIST 1
LIST 2
LIST 3
LIST 4
LIST 5
ALGORITHM A
ALGORITHM B
TRUE RANDOM
GENERATOR BASED
ON CLOCK

FIGURE 6

bank	retailer	tavern	phone company	purchaser	car dealer		other	06432178 Public Information and Recipient
x			x	x				Name: Wayne Stanley
	x	x						Age: 27*
			x	x	x			Date of Birth: 29 March 1973
x								Home Phone: (687) 284-6894
								Work Phone: (312) 684-2641
x			x					e-mail: alex@west.com
x			x					Address: 6824 Fremont Boulevard
x			x					City: Fresno
x			x					State: CA
x								Zip: 98201-3641
x								SSN:
								Middle Name:

x = supply this information to recipient
* = calculated by database management system

FIGURE 7

Numerical Identifier Type	Numercial Identifier	(optional) Uniquness Suffix	Pointer to User's Record
0	503629481		6043289
0	503668821		6059741
0			
0			
1	44 503679418		6079633
1			
1			
1			
2	5426 413268914281	3	6059741
2			
2			
2			

FIGURE 8

Relative Record Number	List of Transactions That Require IDV	Table of IDV's	Public Information and Recipient
6043289	96804294	34682141	06432178
6043290	66432174	39862843	05224101
6043291	88365261	46891300	07891302

FIGURE 9

96804294	
List of Transactions That Require IDV	
All Financial Transactions Except:	
Bank Routing Number XXXX Checking Account Number XXXX Under $50 and ATM Card	Calling Card Number (402) 688-2136 4280

FIGURE 10

34682141

Table of IDV's

IDV	Verification Trans. ID	Time, Date	Requesting Party	Optional Info.
68231	2468	63284987	605886221478	
43801	1890			Check to AYB for $50+
69210	6336	662891478	2246228911876	Credit Card to BNG for $800+
00010	9810			

Attorney Docket No. 13481.1US01

MERCHANT & GOULD P.C.

United States Patent Application

COMBINED DECLARATION AND POWER OF ATTORNEY

As a below named inventor I hereby declare that: my residence, post office address and citizenship are as stated below next to my name; that

I verily believe I am the original, first and sole inventor (if only one name is listed below) or a joint inventor (if plural inventors are named below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: SYSTEM AND METHOD FOR IDENTITY VERIFICATION

The specification of which
a. ☒ is attached hereto
b. ☐ was filed on as application serial no. and was amended on (if applicable) (in the case of a PCT-filed application) described and claimed in international no. filed and as amended on (if any), which I have reviewed and for which I solicit a United States patent.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, § 1.56 (attached hereto).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119/365 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on the basis of which priority is claimed:

a. ☒ no such applications have been filed.
b. ☐ such applications have been filed as follows:

FOREIGN APPLICATION(S), IF ANY, CLAIMING PRIORITY UNDER 35 USC § 119

COUNTRY	APPLICATION NUMBER	DATE OF FILING (day, month, year)	DATE OF ISSUE (day, month, year)

ALL FOREIGN APPLICATION(S), IF ANY, FILED BEFORE THE PRIORITY APPLICATION(S)

COUNTRY	APPLICATION NUMBER	DATE OF FILING (day, month, year)	DATE OF ISSUE (day, month, year)

I hereby claim the benefit under Title 35, United States Code, § 120/365 of any United States and PCT international application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application.

U.S. APPLICATION NUMBER	DATE OF FILING (day, month, year)	STATUS (patented, pending, abandoned)

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below:

U.S. PROVISIONAL APPLICATION NUMBER	DATE OF FILING (Day, Month, Year)
60/157,889	6 October 1999

I hereby appoint the following attorney(s) and/or patent agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith:

Albrecht, John W.	Reg. No. 40,481
Ali, M. Jeffer	Reg. No. 46,359
Anderson, Gregg I.	Reg. No. 28,828
Batzli, Brian H.	Reg. No. 32,960
Beard, John L.	Reg. No. 27,612
Berns, John M.	Reg. No. 43,496
Black, Bruce E.	Reg. No. 41,622
Branch, John W.	Reg. No. 41,633
Bremer, Dennis C.	Reg. No. 40,528
Bruess, Steven C.	Reg. No. 34,130
Byrne, Linda M.	Reg. No. 32,404
Campbell, Keith	Reg. No.P-46,597
Carlson, Alan G.	Reg. No. 25,959
Caspers, Philip P.	Reg. No. 33,227
Chiapetta, James R.	Reg. No. 39,634
Clifford, John A.	Reg. No. 30,247
Daignault, Ronald A.	Reg. No. 25,968
Daley, Dennis R.	Reg. No. 34,994
Dalglish, Leslie E.	Reg. No. 40,579
Daulton, Julie R.	Reg. No. 36,414
DeVries Smith, Katherine M.	Reg. No. 42,157
DiPietro, Mark J.	Reg. No. 28,707
Edell, Robert T.	Reg. No. 20,187
Epp Ryan, Sandra	Reg. No. 39,667
Glance, Robert J.	Reg. No. 40,620
Goggin, Matthew J.	Reg. No. 44,125
Golla, Charles E.	Reg. No. 26,896
Gorman, Alan G.	Reg. No. 38,472
Gould, John D.	Reg. No. 18,223
Gregson, Richard	Reg. No. 41,804
Gresens, John J.	Reg. No. 33,112
Hamer, Samuel A.	Reg. No. P-46,754
Hamre, Curtis B.	Reg. No. 29,165
Harrison, Kevin C.	Reg. No.P-46,759
Hertzberg, Brett A.	Reg. No. 42,660
Hillson, Randall A.	Reg. No. 31,838
Holzer, Jr., Richard J.	Reg. No. 42,668
Johnston, Scott W.	Reg. No. 39,721
Kadievitch, Natalie D.	Reg. No. 34,196
Karjeker, Shaukat	Reg. No. 34,049
Kastelic, Joseph M.	Reg. No. 37,160
Kettelberger, Denise	Reg. No. 33,924
Keys, Jeramie J.	Reg. No. 42,724
Knearl, Homer L.	Reg. No. 21,197
Kowalchyk, Alan W.	Reg. No. 31,535
Kowalchyk, Katherine M.	Reg. No. 36,848
Lacy, Paul E.	Reg. No. 38,946
Larson, James A.	Reg. No. 40,443
Leon, Andrew J.	Reg. No. P-46,869
Leonard, Christopher J.	Reg. No. 41,940
Liepa, Mara E.	Reg. No. 40,066
Lindquist, Timothy A.	Reg. No. 40,701
Lycke, Lawrence E.	Reg. No. 38,540
McAuley, Steven A.	Reg. No. 46,084
McDonald, Daniel W.	Reg. No. 32,044
McIntyre, Jr., William F.	Reg. No. 44,921
Mitchem, M. Todd	Reg. No. 40,731
Mueller, Douglas P.	Reg. No. 30,300
Nichols, A. Shane	Reg. No. 43,836
Pauly, Daniel M.	Reg. No. 40,123
Phillips, Bryan K.	Reg. No. P-46,990
Phillips, John B.	Reg. No. 37,206
Plunkett, Theodore	Reg. No. 37,209
Prendergast, Paul	Reg. No. 46,068
Pytel, Melissa J.	Reg. No. 41,512
Qualey, Terry	Reg. No. 25,148
Reich, John C.	Reg. No. 37,703
Reiland, Earl D.	Reg. No. 25,767
Samuels, Lisa A.	Reg. No. 43,080
Schmaltz, David G.	Reg. No. 39,828
Schuman, Mark D.	Reg. No. 31,197
Schumann, Michael D.	Reg. No. 30,422
Scull, Timothy B.	Reg. No. 42,137
Sebald, Gregory A.	Reg. No. 33,280
Skoog, Mark T.	Reg. No. 40,178
Spellman, Steven J.	Reg. No. 45,124
Stoll-DeBell, Kirstin L.	Reg. No. 43,164
Sumner, John P.	Reg. No. 29,114
Swenson, Erik G.	Reg. No. 45,147
Tellekson, David K.	Reg. No. 32,314
Trembath, Jon R.	Reg. No. 38,344
Tuchman, Ido	Reg. No. 45,924
Underhill, Albert L.	Reg. No. 27,403
Vandenburgh, J. Derek	Reg. No. 32,179
Wahl, John R.	Reg. No. 33,044
Weaver, Karrie G.	Reg. No. 43,245
Welter, Paul A.	Reg. No. 20,890
Whipps, Brian	Reg. No. 43,261
Whitaker, John E.	Reg. No. 42,222
Wickhem, J. Scot	Reg. No. 41,376
Williams, Douglas J.	Reg. No. 27,054
Withers, James D.	Reg. No. 40,376
Witt, Jonelle	Reg. No. 41,980
Wu, Tong	Reg. No. 43,361
Xu, Min S.	Reg. No. 39,536
Zeuli, Anthony R.	Reg. No. 45,255

I hereby authorize them to act and rely on instructions from and communicate directly with the person/assignee/attorney/firm/ organization who/which first sends/sent this case to them and by whom/which I hereby declare that I have consented after full disclosure to be represented unless/until I instruct Merchant & Gould P.C. to the contrary.

Please direct all correspondence in this case to Merchant & Gould P.C. at the address indicated below:

Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903

23552
PATENT TRADEMARK OFFICE

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2	**Full Name Of Inventor**	**Family Name** ELLINGSON	**First Given Name** ROBERT	**Second Given Name** E.
0	**Residence & Citizenship**	**City** WATERTOWN	**State or Foreign Country** SOUTH DAKOTA	**Country of Citizenship** USA
1	**Post Office Address**	**Post Office Address** P.O. BOX 1731	**City** WATERTOWN	**State & Zip Code/Country** SOUTH DAKOTA 57201/USA
Signature of Inventor 201:			**Date:**	

§ 1.56 Duty to disclose information material to patentability.

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is canceled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is canceled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§ 1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) the closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim;

or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application:

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.